April M. Strauss, SBN 163327
astrauss@sfaclp.com
APRIL M. STRAUSS, APC
2500 Hospital Drive, Bldg 3
Mountain View, CA 94040
Phone: (650) 281-7081

William J. Doyle, SBN 188069
bill@doyleapc.com
Chris W. Cantrell, SBN 290874
chris@doyleapc.com
DOYLE APC
550 West B St, 4th Floor
San Diego, CA 92101
Phone: (619) 736-0000

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

JOHN DOE AND JANE DOE, individually and on behalf of all others similarly situated and for the benefit of the public,

Plaintiffs,

vs.

CEREBRAL, INC.,

Defendant.

Case No. 2:23-cv-01828

CLASS ACTION COMPLAINT FOR PRIVACY VIOLATIONS

DEMAND FOR JURY TRIAL

Plaintiffs John Doe and Jane Doe, on behalf of themselves and all others similarly situated, assert the following against Defendant Cerebral, Inc., based upon personal knowledge where so identified and otherwise on information and belief and the investigation of counsel as to all other matters that have evidentiary support or will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

PARTIES

A. Plaintiffs

1. On personal knowledge, Plaintiff Jane Doe ("Plaintiff Jane Doe") is a resident of Aptos, California.

2. On personal knowledge, Plaintiff Jane Doe is a Facebook user and has had a Facebook account during some or all of the relevant period.

3. On personal knowledge, Plaintiff Jane Doe was a registered user of Cerebral and its website, web portal and mobile platform during some or all of the relevant time period.

4. On personal knowledge, to make appointments, track and receive test results, receive medical treatment, and order medications, Plaintiff Jane Doe was required to use the online portals associated with and created by Cerebral.

5. On personal knowledge, Plaintiff Jane Doe's use of Cerebral's patient portals entailed entering her user data, including sensitive medical information such as her identity, treatment, medications, and other highly sensitive personal information.

6. On personal knowledge, Plaintiff Jane Doe received an email from Cerebral, as described below, in early March 2023.

7. On personal knowledge, Plaintiff John Doe ("Plaintiff John Doe") is a resident of Brooklyn, New York.

8. On personal knowledge, Plaintiff John Doe is an Instagram, TikTok and Twitter user and had these accounts during some or all of the relevant time period.

9. On personal knowledge, Plaintiff John Doe was a registered user of Cerebral and its website, web portal and mobile platform during some or all of the relevant time period.

10. On personal knowledge, to make appointments, track and receive test results, receive medical treatment, and order medications, Plaintiff John Doe was required to use the online portals associated with and created by Cerebral.

11. On personal knowledge, Plaintiff John Doe's use of Cerebral's patient portals entailed entering his user data, including sensitive medical information such as his diagnosis of ADHD and anxiety.

12. On personal knowledge, after entering this information on the Cerebral website, Plaintiff John Doe began to receive targeted advertisements related to his private medical information he previously provided Cerebral.

13. On personal knowledge, Plaintiff John Doe received an email from Cerebral, as described below, in early March 2023.

14. Plaintiff Jane Doe and Plaintiff John Doe are referred to herein as "Plaintiffs." Both Plaintiffs created a Cerebral account, completed parts of Cerebral's online mental health self-assessment and/or purchased a subscription plan from Cerebral.

B. Defendant

15. Defendant Cerebral Inc. is a Delaware corporation with its principal place of business located at 340 S. Lemon Ave #9892, Walnut, California 91789.

16. Cerebral operates in and from California through its website at cerebral.com. The company services hundreds of thousands of patients nationwide. It has been valued at $4.8 billion after a $300 million funding round in December 2022.

17. Since 2019, Cerebral has allowed companies like Meta (aka Facebook and Instagram) to surreptitiously collect user data such as provided by Plaintiffs and associate it with Plaintiffs' and other Class Members' Meta accounts for use in targeting

them with advertisements.

JURISDICTION AND VENUE

18. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

19. This Court has general personal jurisdiction over Cerebral because it maintains its principal place of business in California. Additionally, Cerebral is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' and others' claims occurred in or arose out of actions taken in California.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), (c), and (d) because Cerebral is located in this District, transacts business in this District and a substantial portion of the events giving rise to the claims occurred in this District.

STATEMENT OF FACTS

21. To power its advertising business, the social media network Meta Platforms, Inc., doing business as Meta and formerly named Facebook, Inc., and Facebook, Inc. ("Meta") Facebook collects data in a variety of ways. One of these is through its "Meta Pixel" "tracking cookie," which is a small code embedded on third-party websites used to track a users' activity as the users navigate through a website. Meta Pixel can track and log each page a user visits, what buttons they click, and specific information they input into the website.[1]

[1] Meta Business Help Center, About Meta Pixel, https://www.facebook.com/business/help/742478679120153?id=120537668283214 2 (last visited July 13, 2022).

22. Meta Pixel and other online trackers have been incorporated on many health care websites used to store and convey sensitive medical information intended by their users to stay private.

23. Cerebral is a telehealth company based in California that operates through the website cerebral.com. It claims to be "a mental health telemedicine company that is democratizing access to high quality mental health care for all." Cerebral also offers services for those with alcohol dependence and has monthly subscriptions for medication and therapy for mental health conditions, including ADHD, anxiety, and depression. It is reported that Cerebral has served over 200,000 patients nationwide over the last several years. During and since COVID, the number of patients seeking healthcare via Cerebral skyrocketed.

24. Cerebral encourages patients to use its website to research their medical symptoms and health issues, identify doctors who can treat their specific conditions, order, and take other actions related to their personal health care. When doing this, patients convey highly private information, including medical information, through Cerebral's website.

25. As a patient would have to do while visiting any healthcare provider, the new patient would have to disclose a litany of sensitive and confidential information, including the patient's name, address, date of birth, Social Security number, prior medical history, and current symptoms. By inputting this information, patients trusted Cerebral to keep this sensitive and confidential information safe from disclosure to third parties.

26. Cerebral affirmatively included the Meta Pixel and other online trackers on its website, which was done without disclosing this fact to patients.

27. When a user enters health information through Cerebral's website and patient portals that incorporate Meta Pixel and other online trackers, this information—including, in some instances, specifically what the user is seeking treatment for—is sent

to Meta via Meta Pixel and other companies through their online trackers. Particularly in the case of Cerebral, whose function is to work with patients with particular issues such as ADHD, anxiety and depression, companies can obtain a treasure trove of personal medical information about the user simply by those users accessing this site.

28. Third party websites that incorporate Meta Pixel and other online trackers such as operated by Cerebral benefit from the ability to analyze a user's experience and activity on its website to assess the website's functionality and improve traffic. The website also gains information about its customers through the Meta Pixel and other online trackers that can target them with advertisements and measure the results of advertisement efforts. Cerebral transmitted to third parties such as Meta portions of patients' private communications through pieces of tracking code it embedded in its website, solely to share such information with marketing entities.

29. When Meta Pixel and other online trackers are incorporated by companies such as Cerebral, unbeknownst to users and without their consent, unauthorized third parties gain the ability to surreptitiously gather user interaction with the website ranging from what a user clicks on to the personal information entered on a website and later sends users unsolicited advertisements based on that tracking information. This data, which can include health conditions, diagnoses, procedures, treatment status, the treating physician, medications, and other personal information (collectively "User Data"), is viewed, obtained, and used by companies such as Facebook in connection with targeted advertising, either aimed at the Cerebral users themselves or other individuals on social media sites like Facebook, Instagram, TikTok that fit a profile that is continuously being updated by additional personal health information provided by Cerebral through its hidden online trackers.

30. By way of example, Meta's own documentation clarifies just how much the Meta Pixel can track in terms of patients' private information. It describes the MetaPixel as code that Meta's business customers can put on their website to "[m]ake

sure your ads are shown to the right people. Find … people who have visited a specific page or taken a desired action on your website." Meta also instructs such business customers that: "Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads."

31. Plaintiffs had their User Data, including sensitive medical information, harvested through Cerebral's website using the Meta Pixel tool and other online trackers without their consent when they entered information on the patient portal for the Cerebral website, and continued to have their privacy violated when their User Data was used for profit when pharmaceutical and other companies, used the private medical and other information collected to send them targeted advertising related to medical conditions for which they were trying to obtain treatment through Cerebral's website. This information was also monetized by other third parties to reach potential new customers, refine automatic profiling and/or engage in other profit-motivated ventures.

32. Because of this illegal information gathering, Plaintiffs believe Cerebral shared personal health information about then with third parties without their consent, unknowingly providing other third parties with access to this sensitive personal information.

33. Cerebral knows that the User Data collected through the Meta Pixel and other online trackers includes highly sensitive medical information but, in either conscious, reckless or negligent disregard for patient privacy, continued to collect, use, and profit from this information, and by embedding Meta Pixel and other online trackers they were sharing and permitting companies like Meta to collect and use Plaintiffs' and the Class members' User Data, including sensitive medical information.

34. On or about August 19, 2022, Cerebral notified some Cerebral users of a breach of their protected health care information. Several months prior, Cerebral sent certain Cerebral clients a postcard notifying them of the opportunity to participate in a research study. The postcard included the names and addresses of these individuals as well as information regarding the diagnosis, treatment, and the recipient's relationship to Cerebral. However, Cerebral failed to place the postcards in an envelope, thereby exposing the users' confidential health information to public view.

35. In early March 2023, Plaintiffs received notice from Cerebral notifying Plaintiffs of Cerebral's use of tracking technologies on its website which stores a patient's sensitive and confidential information and shares that information with third parties such as Facebook/Instagram. The letter states that on January 3, 2023, after an internal review by Cerebral, that Cerebral determined that it had disclosed protected health information to "certain Third-Party Platforms and some Subcontractors" without notifying Plaintiffs and other class members of this disclosure or obtaining their consent. The letter states that the extent of the protected health information unlawfully disclosed depends upon whether the person simply created a Cerebral account, completed any part of Cerebral's online mental health self-assessment and/or purchased a subscription plan from Cerebral, specifically:

- If you created a Cerebral account, the information disclosed may have included your name, phone number, email address, date of birth, IP address, Cerebral client ID number and other demographic or information;
- If, in addition to creating a Cerebral account, you also completed any part of Cerebral's online mental health self-assessment, the information disclosed may also have included your selected service, assessment responses, and certain associated health information;
- In addition to creating a Cerebral account and completing Cerebral's

> online mental health self-assessment, if one also purchased a subscription plan from Cerebral, the information disclosed may have included subscription plan type, appointment dates and other booking information, treatment and other clinical information, health insurance/pharmacy benefit information (for example, health plan name, group/member numbers, and insurance co-pay amounts).

36. Cerebral's March 2023, letter states that "[u]pon learning of this issue, Cerebral promptly disabled, reconfigured and/or removed the Tracking Technologies on Cerebral's Platforms to prevent any such disclosures in the future and discontinued or disabled data sharing with any Subcontractors not able to meet all HIPAA requirements." This is likely not true being that a U.S. Senate investigation a month earlier had at least partially revealed Cerebral's illegal conduct, as referenced below.

37. Defendant's actions constitute an extreme invasion of Plaintiffs and Class members' right to privacy and violate various federal and state statutes and common law doctrines, including the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631, *et seq*. and the privacy rights protected by California's Constitution and common law; violation of California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq*.; violation of California's Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.; breach of fiduciary duty, and other tortious acts as described herein.

A. Background of California Laws Protecting Privacy

38. In California, the protection of personal privacy is of paramount importance. Article 1, section 1 of the California Constitution guarantees consumers a right of privacy. In addition, as recognized by the California State Legislature, using computer information technology has greatly magnified the potential risk to individual privacy that occurs from the maintenance of personal information by entities such as Defendant, requiring the maintenance of personal information to be subject to strict

limits as set out in many California statutes.

39. Under California law, medical information is considered among the most sensitive private personal information available. "Medical Information" is defined by California's Confidential Medical Information Act, Cal. Civ. Code sections 56, et seq. ("CMIA") as:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.

40. "Individually identifiable" means that the Medical Information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security Number, or other information that, alone or combined with other publicly available information, reveals the identity of the individual.

41. "Personal and Medical Information", for purposes of this Complaint, refers to the above definition and encompasses both Personal Health Information ("PHI"), and Personally Identifiable Information ("PII"), including information associated with individual's health maintained within Cerebral's computer systems.

42. Since Personal and Medical Information encompasses such sensitive and revealing information, it is highly valued. Personal and Medical Information has been found to command up to $1,000 per individual record.

43. Under the CMIA and other laws Plaintiffs and Class members have a recognized right to confidentiality in their Personal and Medical Information and can reasonably expect that their Personal and Medical Information would be protected by Defendant from unauthorized access. When Plaintiffs and Class members provided their Personal and Medical Information to Cerebral for enrollment, maintaining an

account with Cerebral, seeking coverage for medical treatment and otherwise availing themselves of healthcare services through Cerebral, they did so with the reasonable understanding and assurance that their Personal and Medical Information would be kept confidential and secure.

44. The Historical and Statutory Notes for the short title of the CMIA, § 56, support these reasonable expectations:

> The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable Medical Information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable Medical Information, while permitting certain reasonable and limited uses of that information.

Stats. 1981, ch. 782, § 1, p. 3040.

45. Consistent with that statutory purpose, the CMIA states that "a provider of health care, health care service plan, or contractor shall not disclose Medical Information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization [. . .]." Cal. Civ. Code § 56.10(a). Defendant's actions in such a capacity permitted the disclosure of the Personal and Medical Information at issue here to unauthorized third parties.

46. Additionally, Cal. Civ. Code § 56.101(a) states, in relevant part, that every health care provider, health care service plan or health care contractor that creates, maintains, preserves, or stores Personal and Medical Information shall do so in a manner that preserves its confidentiality. Defendant's actions establish that they did not maintain the Personal and Medical Information at issue in a manner that preserved its confidentiality. Cerebral's failure to create, maintain, preserve, and store Personal and Medical Information in a manner that preserved the confidentiality of the information contained therein resulted in the illegal access, authorization, exfiltration, disclosure,

and negligent release of well over 200,000 personal unique records, which included Personal and Medical Information, to known third parties such as Meta.

B. A Senate Investigation Reveals Cerebral's Disclosure of Sensitive User Data

47. On February 2, 2023, two members of the United States Senate sent a letter to Cerebral where they "express our concern regarding reports that Cerebral is tracking and sharing sensitive and personally-identifiable health data with third-party social media and online search platforms such as Google and Facebook that monetize this data to target advertisements" using the Meta Pixel tracking code. What was of particular concern is that Cerebral's website was used by over 200,000 patients in 2020 and 2021 alone.

48. On Cerebral's website, patients are asked to answer questions covering conditions such as depression, anxiety, and bipolar disorder. Although Cerebral's website claims that information entered on these intake forms is confidential and secure, this information is sent to advertising platforms such as Facebook, along with the information needed to identify users. This data is extremely personal, and it can be used to target advertisements for services that may be unnecessary, or that according to the U.S. Senate letter may be "potentially harmful physically, psychologically, or emotionally."

49. On November 30, 2022, a spokesperson for Cerebral wrote in an email to Senate investigators, "We are removing any personally identifiable information, including name, date of birth, and zip code from being collected by the Meta Pixel," effectively admitting that before that date it was providing third party advertisers such as Meta with access to that information. However, as late as December 7, 2022, it was reported by the Senate investigatory letter that Cerebral's website was still collecting personally identifiable information. Tracking such private information also could reveal sensitive and personal material leading to other forms of privacy and security breaches.

50. This is not the first allegation of privacy related issues made against Cerebral. In a lawsuit filed in California state court in April 2022, a former Cerebral employee alleged he was fired in retaliation for objecting to the company's plans to "egregiously put profits and growth before patient safety" after he raised several concerns to Cerebral leadership during his time at the company. The Complaint also alleges that Cerebral does not adhere to regulations with respect to the privacy and security of patient data, and specifically that "employees and former employees could gain unauthorized access to confidential patient medical information," potentially compromising tens of thousands of patient records. And back on August 19, 2022, a related medical provider group Cerebral Medical Group, P.A. notified the U.S. Department of Health and Human Services about a security breach incident involving over 6,100 patients stemming from an unauthorized access and disclosure of certain types of patient information.

51. The federal government recently issued a warning to companies such as Cerebral that tracking code like Meta Pixel and other third party trackers may violate federal privacy laws when installed on healthcare websites. The statement, titled *Use of Online Tracking Technologies By HIPAA Covered Entities And Business Associates* (the "Bulletin"), was recently issued by the Department of Health and Human Services' Office for Civil Rights ("OCR"). While healthcare organizations regulated under HIPAA may use third-party tracking tools in a limited way, such as to analyze data key to its operations, they may not use these tools to expose patients' protected health information to third party marketers. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.

52. The Bulletin also identified the types of harm that disclosure may cause to

the patient:

> "An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule."

53. Plaintiffs and Class members had no idea that Defendant was collecting and using their User Data, including sensitive medical information, when they engaged with Cerebral's sites that incorporate Meta Pixel and other online trackers because the software code is hidden from users.

54. For example, when Plaintiffs logged into Cerebral's patient portal, there was no indication or disclosure that Meta Pixel was active, embedded in the page, or that it would collect their sensitive medical information.

55. Plaintiffs and all Class members, could not consent to Defendant's conduct when they were unaware their sensitive medical information would be collected and used.

56. By how Meta Pixel and other online trackers work, Cerebral was aware that by incorporating these online trackers onto its website doing so would result in the disclosure and use of Plaintiffs' and Class members' personal information, including sensitive medical information. As it never disclosed the presence of the Meta Pixel or other invisible online trackers, Defendant did not obtain users' consent to collect, use,

and store Plaintiffs' and Class members' sensitive medical information.

C. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy regarding their Sensitive Medical Information

57. Plaintiffs and Class members have a reasonable expectation of privacy in their User Data, including personal information and sensitive medical information. Defendant surreptitiously collected, used, and disclosed Plaintiffs and Class members' User Data, including, highly sensitive medical information, through Meta Pixel and other online trackers in violation of Plaintiffs' and Class members' reasonable expectations of privacy.

58. Privacy polls and studies show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data, and thus disclosure of such practices would be material to them. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data collected about them.[2] According to a study by Pew Research Center, approximately 79% of Americans are concerned about how data is collected about them by companies.[3]

59. The concern about sharing medical information is compounded by the reality that advertisers view this information as having a particularly high value. Having

---

[2] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[3] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

access to the data women share with their healthcare providers lets advertisers obtain data on children before they are even born. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[4] The article continues "Children today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[5]

60. Defendant is required by the CMIA and other California laws identified, and various other laws and regulations to protect Plaintiffs' and Class members' Personal and Medical Information and to handle notification of any breach in accordance with applicable breach notification statutes. These duties are established in many California statutes, including Cal. Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29, Cal. Bus. and Prof. Code §§ 17200 et seq., Cal. Bus. and Prof. Code §§ 22575-2257, Cal. Penal Code § 630-632 et seq., and Article I, § 1 of the California Constitution. Failing to do so results in acts of negligence *per se* by Defendant.

61. In addition, as Defendant is an entity covered by HIPAA and various contracts require they do so, they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards

---

[4] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, The MIT Press Reader, https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

[5] *Id.*

and duties for Defendant's protection of Personal and Medical Information maintained by them in electronic form. HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. See 45 C.F.R. § 164.502. HIPAA also requires that covered entities implement safeguards to protect this information. See 45 C.F.R. § 164.530(c)(1).

62. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

63. "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

64. HIPAA's Security Rule requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably expected threats or hazards to the security or integrity of such information; (c) protect against any reasonably expected uses or disclosures of such information that are not permitted; and (d) ensure compliance by their workforce.

65. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

66. Defendant failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to:

(a) Failed to ensure the confidentiality and integrity of electronic PHI

that Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failed to put technical policies and procedures into practice for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failed to put policies and procedures into practice to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failed to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failed to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failed to protect against any reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failed to ensure compliance with HIPAA security standard rules by its workforce by providing for adequate comprehensive training rather than simply using training software to test staff by imitating phishing emails, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly used and disclosed PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failed to effectively train all members of its workforce (including

independent contractors) on the policies and procedures for PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI beyond simply using training software to test staff by imitating phishing emails, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

(j) Failed to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with violation of 45 C.F.R. section 164.530(c).

67. Defendant also violated the duties applicable to them under the Federal Trade Commission Act, 15 U.S.C. § 45 et seq. ("FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

68. As established by these laws, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in their possession from being misused by unauthorized persons such as Meta and other unauthorized third parties. This also included a duty to Plaintiffs and Class members to design, maintain, and test their computer systems to make sure the Personal and Medical Information in their possession was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession; and to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information.

69. By taking affirmative acts inconsistent with these obligations, Defendant disclosed and permitted the disclosure of Personal and Medical Information to unauthorized third parties, including Meta and other unauthorized third parties.

Through such actions or inactions, Cerebral failed to preserve the confidentiality of Personal and Medical Information they were duty-bound to protect.

70. As a direct and proximate result of Defendant's actions, inactions, omissions, breaches of duties and want of ordinary care that directly and proximately caused or resulted in this unauthorized disclosure, Plaintiffs and Class members have suffered and will continue to suffer damages and other injury and harm in the form of, inter alia, (a) invasion of privacy, (b) breach of the confidentiality of their Personal and Medical Information, (c) deprivation of the value of their PHI, for which there is a well-established national and international market, as well as statutory damages to which they are entitled even without proof of access or actual damages; and (d) increased risk of future harm.

D. The Value of Personal and Medical Information Shows Plaintiffs and Class Members Lost Money or Property

71. It is well known that Personal and Medical Information is a valuable commodity such that Plaintiffs and Class members would lose money or property if their sensitive health data was improperly accessed and disclosed.

72. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person, depending upon completeness. PII and PHI can be sold at a price ranging from approximately $20 to $300.

73. Time Magazine in an article titled *How Your Medical Data Fuels A Hidden Multi-Billion Dollar Industry*, referenced the "growth of the big health data bazaar," in which patients' health information is sold. It reported that: "[T]he secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future."

TOLLING, CONCEALMENT, AND ESTOPPEL

74. The applicable statutes of limitation have been tolled because of Defendant's knowing and active concealment and denial of the facts alleged.

75. Defendant incorporated Meta Pixel and other third party trackers into the Cerebral website, concealing from consumers that they were interacting with a website with the Meta Pixel tracker and other third party trackers enabled.

76. Defendant had exclusive knowledge of this material fact yet failed to disclose that by interacting with a website that Plaintiffs' and Class members' sensitive medical information would be collected, used, and stored by unauthorized third party marketers.

77. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Defendant's conduct, including because there were no disclosures or other indications they were interacting with a website that Plaintiffs' and Class members' sensitive medical information would be collected, used, and stored by unauthorized third party marketers.

78. The earliest Plaintiffs and Class members, acting with due diligence, could have reasonably discovered this conduct would have been on February 2, 2023, when the Senate's investigation was publicly disclosed.

79. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Under the circumstances, Defendant was under a duty to disclose the nature and significance of these data collection practices but failed to do so. Defendant is therefore estopped from relying on any potentially applicable statute of limitations.

CLASS ACTION ALLEGATIONS

80. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2) and/or (b)(3) individually and on behalf of the following Class:

All natural persons in the United States whose User Data were collected

through third-party tracking technology from any Cerebral website since January 1, 2019.

81. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel and Defendant's counsel.

82. The exact number of members of the Class is unknown and unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The Class likely consists of over 200,000 individuals, and the members can be identified through Cerebral's records.

83. The Class's claims present common questions of law and fact, and those questions predominate over questions that may affect individual Class members. Common questions for the Class include, but are not limited to:

- Whether Defendant implemented and maintained reasonable security practices and procedures appropriate to protect Plaintiffs' and Class members' Personal and Medical Information from unauthorized access or disclosure.
- Whether Defendant and its employees, agents, officers, or directors negligently or unlawfully disclosed or permitted the unauthorized disclosure of Plaintiffs' and Class members' Personal and Medical Information to unauthorized persons.
- Whether Defendant negligently created, maintained, preserved, stored, abandoned, or disposed of Plaintiffs' and Class members' Personal and Medical Information, and failed to protect and preserve the integrity of the Personal and Medical Information found on Cerebral's electronic

systems.

- Whether Defendant's actions or inactions were a proximate result of the negligent or reckless release of confidential information or records about Plaintiffs and the Class.
- Whether Defendant has adequately addressed and fixed the websites that enabled the collection and disclosure of their Personal and Medical Information.
- Whether Defendant engaged in "unfair" business practices by failing to safeguard the Personal and Medical Information of Plaintiffs and the Class, and whether Defendant's violations of the state and federal laws cited are "unlawful" business practices in violation of California Business and Professions Code § 17200, *et seq*.
- Whether Defendant violated the California Medical Information Act, the California Invasion of Privacy Act, and the other laws cited.
- Whether Plaintiffs and the Class are entitled to damages, equitable and injunctive relief to redress the imminent and ongoing harm faced because of this unauthorized disclosure and Defendant's failure to provide full and adequate notice of it, and the scope of such relief.

84. Plaintiffs' claims are typical of the claims of the other members of the Class. The claims of Plaintiffs and the members of the Class arise from the same conduct by Defendant and are based on the same legal theories.

85. Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiffs retained counsel competent and experienced in complex litigation and class actions, including litigation to remedy privacy violations. Plaintiffs have no interest materially antagonistic to the interests of the Class, and Defendant has no defenses unique to any Plaintiffs. Plaintiffs and counsel are committed to vigorously prosecuting this action on behalf of the members of the Class,

and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest materially adverse to the interests of the other members of the Class.

86. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable.

87. Pursuant to Rule 23(b)(3), in consideration of (a) the class members' interests in individually controlling the prosecution or defense of separate actions (which in light of the statutory damages may not be significant); (b) the extent and nature of any litigation concerning the controversy already begun by or against class members (of which Plaintiffs are not aware of any such litigation); (c) the desirability or undesirability of concentrating the litigation of the claims in the particular forum (here, where Defendant's headquarters are based); and (d) the likely difficulties in managing a class action (which considering the common issues involved should not be significant), this proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

88. As Cerebral has contact information for Plaintiffs and Class members and recently sent an electronic notice to them as set forth above, notice of the pendency of this action can be accomplished via electronic mail to all members of the proposed Class.

89. Plaintiffs reserve the right to revise the class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

90. California substantive laws apply to every member of the Class. California's substantive laws may be constitutionally applied to the claims of Plaintiffs

and the Class under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiffs and Class members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

91. Cerebral's principal place of business is located in this District and it conducts substantial business in California, such that California has an interest in regulating Cerebral's conduct under its laws. Cerebral's decision to reside in California and avail itself of California's laws renders the application of California law to the claims herein constitutionally permissible. The conduct at issue also originated in and emanated from California as that is where the decisions to include the Meta Pixel and other third-party trackers were made and likely effectuated, and where the illegal data transfers took place. Defendant communicated with Meta and other unauthorized third parties while this User Data was in transit or was being sent from or received within California through servers maintained by either Defendant or third parties in this State.

92. Applying California law to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of the Plaintiffs and the proposed Class, at least one of the Plaintiffs and many Class members reside in this State, and California has a greater interest in applying its laws here than any other interested state.

COUNT 1

Violation of the Confidentiality of Medical Information Act

(Cal. Civ. Code § 56 *et seq.*)

93. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

94. Defendant is a "health care service plan", "provider of health care"

and/or a "recipient" of Personal and Medical Information as defined by Cal. Civ. Code § 56.05(d) and (m), § 56.06(a), (b) & (d) and/or Section 56.13 and therefore subject to the requirements of the CMIA.

95. California Civil Code § 56.06(d) specifically provides that (d) "[a]ny business that offers a mental health digital service to a consumer for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part."

96. Defendant must not disclose or permit the disclosure of Personal and Medical Information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining authorization, subject to certain exceptions found in Cal. Civ. Code §§ 56.10(b) & (c) that do not apply here. Cal. Civ. Code § 56.10(a). By their affirmative acts and inactions set forth above, Defendant disclosed or permitted the disclosure of Personal and Medical Information to unauthorized third parties, in violation of this Section.

97. Defendant is required under the CMIA to ensure that it maintains, preserves, and stores Personal and Medical Information in a manner that preserves the confidentiality of the information contained therein. Cal. Civ. Code §§ 56.101(a) & 56.36(b).

98. Defendant is required to create, maintain, preserve, store, abandon, or dispose of Personal and Medical Information in a non-negligent manner. Cal. Civ. Code § 56.101(a).

99. Defendant's electronic health record systems or electronic medical record systems are required to protect and preserve the integrity of electronic Personal and Medical Information. Cal. Civ. Code § 56.101(b)(1)(A). The term "electronic health record" or "electronic medical record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by

authorized health care clinicians and staff. Cal. Civ. Code § 56.101(c) as defined by 42 U.S.C. § 17921(5).

100. Plaintiffs and members of the Class are "Patients" as defined by Cal. Civ. Code section 56.05(j).

101. A significant portion of the information at issue in this action is "Medical Information" as that term is defined by § 56.05(i) of the CMIA.

102. As described above, the actions or inactions of Defendant failed to preserve the confidentiality of Personal and Medical Information, including but not limited to Plaintiffs' and Class members' full names, dates of birth, addresses, Social Security numbers, as well as likely insurance provider information, and participant information that, either alone or in combination with other publicly available information, reveals their identities.

103. The Meta Pixel tracking code and those used by other third parties made possible the linking of a Cerebral website user and their identity. The information exchanged, including the contents of searches and the act and substance of ordering medications and other services provided on the Cerebral website, and even the mere use of that website in light of the services offered, reveals information about patients' "physical condition or history."

104. As a result of placing the Meta Pixel and other tracking software on its website, Defendant has released, disclosed, and/or negligently allowed third parties that are known to Defendant, including Meta and other unauthorized third parties, to access and view Plaintiffs' and Class members' medical information without first obtaining their written authorization as required by the provisions of Civil Code § 56, et seq.

105. As a further result of the Defendant's actions, the confidential nature of the Plaintiffs' and Class members' medical information was breached due to Defendant's negligence or affirmative decisions.

106. The Personal and Medical Information was accessed, removed, and

viewed by unauthorized third parties including Meta and other unauthorized parties by virtue of the Meta Pixel and other tracking software embedded in Cerebral's website.

107. In violation of the CMIA, Defendant disclosed or permitted the disclosure of Personal and Medical Information regarding Plaintiffs and Class members without authorization to a third party. This disclosure did not qualify for any of the exemptions set forth in Cal. Civ. Code §§ 56.10(b) or (c), which provide limited bases for allowing unauthorized disclosures. This disclosure of Personal and Medical Information to unauthorized individuals resulted from the affirmative actions and inactions of Defendant.

108. In violation of the CMIA, Defendant created, maintained, preserved, stored, abandoned, or disposed of Personal and Medical Information of Plaintiffs and Class members in a manner that did not preserve the confidentiality of the information contained therein.

109. In violation of the CMIA, Defendant negligently created, maintained, preserved, stored, abandoned, or disposed of Personal and Medical Information of Plaintiffs and Class members.

110. In violation of the CMIA, Defendant's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiffs' and Class members' Personal and Medical Information.

111. In violation of the CMIA, Defendant negligently released confidential or medical information or records concerning Plaintiffs and Class members. Defendant also violated § 56.101(a) of the CMIA.

112. In violation of the CMIA, as a recipient of medical information pursuant to an authorization it disclosed and/or permitted the disclosure of that medical information without obtaining a new authorization that meets the requirements of Section 56.11, or as specifically required or permitted by law.

113. As a direct and proximate result of Defendant's wrongful actions,

inactions, omissions, and want of ordinary care that directly and proximately caused the release of Personal and Medical Information of hundreds of thousands of individuals, such Personal and Medical Information was viewed by, released to, and disclosed to third parties without appropriate written authorization.

114. Plaintiffs and Class members are therefore entitled to injunctive relief and reasonable attorneys' fees and costs.

115. Plaintiffs seek actual damages for Class members, statutory damages of $1,000 per Class member and punitive damages of $3,000 per Class member. In order to recover under the CMIA, Civil Code Section 56.36 expressly states that it is not necessary that the plaintiffs suffered or were threatened with actual damages.

COUNT 2

Violation of the California Invasion of Privacy Act

(Cal. Penal Code §§ 630, 631, et seq. ("CIPA"))

116. Plaintiffs incorporate the foregoing allegations as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

117. California's Invasion of Privacy Act, California Penal Code 631(a) provides a remedy against, *inter alia*: "Any person who … intentionally taps, or makes any unauthorized connection, whether physically, electrically, …, or otherwise, with any telegraph or telephone wire, line, cable, or instrument … or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

118. Defendant Cerebral is a person for the purposes of this law.

119. Defendant "intentionally tap[ped] … or ma[de] [an] unauthorized connection" with respect to Class members' communications by placing third party tracking code on its website, without "the consent of all parties" including Plaintiffs, and thereby violated the CIPA.

120. Defendant also "aid[ed], agree[d] with, employ[d], or conspire[d] with" Meta and other third parties providing marketing services by placing their third-party tracking code on its website, and allowing such entities; to "tap" communications on its website without "the consent of all parties" including Plaintiffs, and thereby violated CIPA.

121. Defendant facilitated the interception and simultaneous transmission to Meta and others of Plaintiffs' and other Class members' PII and PHI while the information was "in transit." As Plaintiffs and Class members typed communications into Defendant's website, as a result of the Meta Pixel and other tracking codes that Defendant placed there, their requests were simultaneously redirected to Meta and other unauthorized third parties while they were still on their way to Defendant.

122. The information communicated between patients and Cerebral was transmitted to and/or from the State of California. The information was wiretapped "while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state."

123. Redirection of data as a result of tracker coding before that data reaches its originally intended recipient (here, Cerebral) does not constitute a separate communication for the purposes of exclusion from CIPA coverage.

124. Cerebral enabled non-parties to the communications to "read" the communications for the purposes of the statute. For example, Meta and other unauthorized third parties could see which individuals searched for specific issues, what conditions they researched, and when and where they made appointments.

125. Cerebral facilitated this communication "without authorization" of Plaintiffs and Class members because it did not give them any hint that the transmission was happening.

126. Plaintiffs and Class members did not request that Defendant and third parties target them with advertising that might be related to their health conditions.

127. Cal. Penal Code § 637.2(a) provides that any person who has been injured by a violation of this chapter [including Penal Code §§ 630 and 631] may bring an action against the person who committed the violation for the greater of the following amounts:

(a) Five thousand dollars ($5,000) per violation.

(b) Three times the amount of actual damages, if any, sustained by the plaintiff.

128. Section 637.2(b) provides that "[a]ny person may . . . bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided by subdivision (a)." Cal. Penal Code § 637.2(b).

129. Section 637.2(c) provides, "It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages." Cal. Penal Code § 637.2(c).

130. Defendant is therefore liable to Plaintiffs and the Class for, at a minimum, statutory damages of $5,000 per violation as well as actual damages, and Plaintiffs and Class members are also entitled to injunctive relief.

COUNT 3

Violation of the California Invasion of Privacy Act

(Cal. Penal Code § 632, *et seq.*)

131. Plaintiffs incorporate the foregoing allegations as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

132. Cal. Penal Code § 632 provides, in relevant part, that it is unlawful to

"intentionally and without the consent of all parties to a confidential communication," "use[] [a] recording device to … record the confidential communication." As used in the statute "'confidential communication' means any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto."

133. The written transmission of information about Plaintiffs' and Class members' searches and clicks on Cerebral's website as described above is a recording of those communications.

134. The Meta Pixel code and the code of other third party tracking services included by Cerebral on its website is a "recording device."

135. Defendant did not have Plaintiffs' or other Class members' express authorization or consent to record their communications. Cal. Penal Code § 637.2(a) provides that any person who has been injured by a violation of this chapter [including Penal Code § 632] may bring an action against the person who committed the violation for the greater of the following amounts:

(a) Five thousand dollars ($5,000) per violation.

(b) Three times the amount of actual damages, if any, sustained by the plaintiff.

136. Section 637.2(b) provides that "[a]ny person may . . . bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided by subdivision (a)." Cal. Penal Code § 637.2(b)

137. Section 637.2(c) provides, "It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages." Cal. Penal Code § 637.2(c).

138. Defendant is therefore liable to Plaintiffs and the Class for, at a minimum, statutory damages of $5,000 per violation, and actual damages. Plaintiffs and Class members are also entitled to injunctive relief.

COUNT 4

Invasion of Privacy

(California Constitution, Article I, Section 1)

139. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

140. The California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I., § 1.

141. Plaintiffs and Class members had a legitimate expectation of privacy in their Personal and Medical Information, and were entitled to the protection of this information against disclosure to unauthorized third parties.

142. Defendant owed a duty to Plaintiffs and Class members to keep their Personal and Medical Information confidential.

143. Defendant failed to protect and released to unauthorized third parties the Personal and Medical Information of Plaintiffs and Class members.

144. Defendant allowed unauthorized third parties such as Meta access to and examination of the Personal and Medical Information of Plaintiffs and Class members by way of Defendant's affirmative actions and negligent failures to protect this information.

145. The unauthorized release to, custody of, and examination by unauthorized third parties of the Personal and Medical Information of Plaintiffs and Class members is highly offensive to a reasonable person.

146. The intrusion at issue was into a place or thing, which was private and is entitled to be private.

147. Plaintiffs and Class members disclosed their Personal and Medical

Information to Defendant as part of Plaintiffs' and Class members' relationships with Defendant, but privately and with the intention that the Personal and Medical Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization or affirmative consent.

148. The sharing of data that resulted from the actions and inactions of Defendant constitutes an intentional interference with Plaintiffs' and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns and those of their families, of a kind that would be highly offensive to a reasonable person.

149. Defendant either knew or reasonably should have known that its inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class members.

150. As a proximate result of the above acts and omissions of Defendant, the Personal and Medical Information of Plaintiffs and Class members was disclosed to third parties without authorization, causing Plaintiffs and Class members to suffer injuries and damages.

151. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and the Class, entitling them to seek injunctive relief. Plaintiffs also seek damages to the fullest extent permitted by law.

152. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiffs in relation to Plaintiffs' stake in the matter. Because this case is brought for the purposes of enforcing

important rights affecting the public interest, Plaintiffs also seek the recovery of attorneys' fees and costs in prosecuting this action against Defendant under Cal. Code Civ. Proc. § 1021.5 and other applicable law.

COUNT 5

Negligence and Negligence Per Se

153. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

154. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class members' Personal and Medical Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, misused, and disclosed to unauthorized parties.

155. As a provider of health care under the law, Defendant had a special relationship with Plaintiffs and Class members who entrusted Defendant with adequately protecting their Personal and Medical Information.

156. Defendant knew that the Personal and Medical Information at issue was private and confidential and should be protected as private and confidential, and thus, Defendant owed a duty of care not to subject Plaintiffs and Class members to an unreasonable risk of unauthorized disclosure.

157. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal and Medical Information and allowing it to be accessed by unauthorized third parties.

158. Defendant's failure to take proper security measures to protect Plaintiffs and Class member's Personal and Medical Information created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of Personal and Medical Information by unauthorized third parties. As described above, Plaintiffs and Class members are part of a foreseeable, discernable

group that was at high risk of having their Personal and Medical Information compromised, and otherwise wrongly disclosed if not adequately protected by Defendant.

159. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class members' Personal and Medical Information.

160. Defendant had a duty to employ reasonable security measures, systems, processes, and otherwise protect the Personal and Medical Information of Plaintiffs and Class members pursuant to the state and federal laws set forth above, resulting in Defendant's liability under principles of negligence and negligence per se.

161. Defendant owed a duty to timely and adequately inform Plaintiffs and Class members, in the event of their Personal and Medical Information being improperly disclosed to unauthorized third parties.

162. Defendant systematically failed to provide adequate security for data in their possession or over which they had supervision and control.

163. Defendant, through its actions and omissions, unlawfully breached duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class members' Personal and Medical Information within Defendant's possession, supervision, and control.

164. Defendant, through its actions and omissions, unlawfully breached duties owed to Plaintiffs and Class members by failing to have appropriate procedures in place to prevent dissemination of Plaintiffs' and Class members' Personal and Medical Information.

165. Defendant, through their actions and omissions, unlawfully breached duties to timely and fully disclose to Plaintiffs and Class members that the Personal and Medical Information within Defendant's possession, supervision, and control was improperly accessed by unauthorized third parties, the nature of this access, and

precisely the type of information improperly accessed.

166. Defendant's breach of duties owed to Plaintiffs and Class members proximately caused Plaintiffs' and Class members' Personal and Medical Information to be compromised by being accessed by unauthorized third parties.

167. As a result of Defendant's ongoing failure to adequately notify Plaintiffs and Class members regarding what type of Personal and Medical Information has been compromised, Plaintiffs and Class members are unable to take the necessary precautions to mitigate damages.

168. Pursuant to the laws set forth herein, including Cal. Civ. Code s§ 56.10(a), 56.101, 1798.21, 1798.29 and Article I, § 1 of the California Constitution. Defendant also violated federal statutes and regulations, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class members' Personal and Medical Information.

169. Plaintiffs and Class members are within the class of persons that these statutes and rules were designed to protect.

170. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class members' Personal and Medical Information in compliance with applicable laws would result in an unauthorized third-party such as Meta gaining access to Plaintiffs' and Class members' Personal and Medical Information, resulting in Defendant's liability under principles of negligence per se.

171. Plaintiffs' and Class members' Personal and Medical Information

constitutes personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiffs and Class members.

172. As a proximate result of Defendant's negligence and breach of duties as set forth above, Defendant's breaches of duty caused Plaintiffs and Class members to, inter alia, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their Personal and Medical Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Personal and Medical Information, all of which can constitute actionable actual damages.

173. In failing to secure Plaintiffs' and Class members' Personal and Medical Information, Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class members' rights. Plaintiffs, in addition to seeking actual damages, also seek punitive damages on behalf of themselves and the Class.

174. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class members' Personal and Medical Information, and as a result, Plaintiffs and Class members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence and negligence *per se*.

COUNT 6

Breach of Fiduciary Duty

175. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

176. Plaintiffs and Class members gave Defendant their Personal and Medical Information in confidence, believing that Defendant would protect that information. Plaintiffs and Class members would not have provided Defendant with this information had they known it would not be adequately protected and would be misused by Defendant.

177. Defendant's acceptance and storage of Plaintiffs' and Class members' Personal and Medical Information created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light of this relationship, Defendant must act primarily for the benefit of its members, which includes safeguarding and protecting Plaintiffs' and Class Members' Personal and Medical Information.

178. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly safeguard Plaintiffs' and Class members' Personal and Medical Information that it collected.

179. As a direct and proximate result of Defendant's breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity compromise to unauthorized third parties; (ii) the loss of the opportunity to determine when and how their Personal and Medical Information is used; (iii) the compromise and publication of their Personal and Medical Information to unauthorized third parties; and (iv) the continued risk to their Personal and Medical Information, which remain in Defendant's possession, custody or control and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate

and adequate measures to protect the Personal and Medical Information of current and former patients and their beneficiaries and dependents.

COUNT 7

Violation of California's Unfair Competition Law

(Cal. Bus. & Prof. Code §§ 17200 *et seq.*)

180. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder, except as to entitlement to and claims for damages, which are not sought in this Cause of Action.

181. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendant as alleged herein constituted unlawful and unfair business acts and practices within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq*.

182. Defendant engaged in "unlawful" business acts and practices in violation of the California statutes set forth above, including Cal. Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29 and Article I, § 1 of the California Constitution, the Online Privacy Protection Act, California Business and Professions Code §§ 22575-22579 ("CalOPPA"), the California Invasion of Privacy Act, and Cal. Penal Code § 630-632 et seq. ("CIPA"). Defendant's acts and practices detailed above also violated federal statutes and regulations, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above. Plaintiffs reserve the right to allege other violations of law committed by Defendant that constitute unlawful business acts or practices within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq*. The allegations of facts set forth in detail above specifically describe and demonstrate how Defendant's actions and inactions violated these laws.

183. Defendant has also engaged in "unfair" business acts or practices. There are several tests that determine whether a practice that impacts consumers as compared to competitors is "unfair," examining the practice's impact on the public balanced against the reasons, justifications and motives of Defendant. Defendant's conduct would qualify as "unfair" under any of these standards:

(a) whether the practice offends an established public policy, which here is whether the practices at issue offend the policies of protecting consumers' Personal and Medical Information by engaging in illegal practices, as reflected in California law and policy set forth above;

(b) balancing the utility of Defendant's conduct against the gravity of the harm created by that conduct, including whether Defendant's practices caused substantial injury to consumers with little to no countervailing legitimate benefit that could not reasonably have been avoided by the consumers themselves, and causes substantial injury to them; or

(c) whether the practice is immoral, unethical, oppressive, unscrupulous, unconscionable or substantially injurious to consumers.

184. The unfair business practice and harm caused by Defendant's failure to maintain adequate information security procedures and practices, including, but not limited to, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized disclosures, failing to properly and adequately educate and train employees, failing to put into place reasonable or adequately protected computer systems and security practices to safeguard patients' Personal and Medical Information, improperly installing code that would permit access to unauthorized persons and thus failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the Personal and Medical Information of Plaintiffs and the Class members in their possession, and failing to protect and preserve confidentiality of Personal and Medical Information of Plaintiffs and Class members

against disclosure and release, outweighs the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, and offensive, and causes substantial injury to Plaintiffs and Class members. The allegations of facts set forth in detail above specifically describe and demonstrate how Defendant's actions and inactions constitute unfair business practices.

185. Defendant either knew or should have known that Cerebral's data security and protection practices were inadequate to safeguard the Personal and Medical Information of Plaintiffs and Class members. The business acts and practices by Defendant for failure to keep confidential medical, or personal data protected did not meet all applicable standards of care and vigilance.

186. These unlawful and unfair business acts or practices conducted by Defendant have been committed in the past and continue. While Defendant has acknowledged some of the wrongful nature of its actions, Defendant has not fully corrected or publicly issued comprehensive corrective notices to Plaintiffs and the Class members and may not have fully corrected or enacted adequate policies and procedures to protect and preserve the confidentiality of medical and personal identifying information of Plaintiffs and the Class members in Defendant's possession and in the possession of unauthorized third parties.

187. As set forth above, Plaintiffs and Class members have been injured in fact and lost money or property as a result of Defendant's unlawful and unfair business practices, having lost control over information about them that has a specific inherent monetary value that can be sold, bartered, or exchanged. In addition, Plaintiffs and Class members have suffered injury in fact and a loss of money or property by at least the following: (i) suffering actual identity compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used; (iii) the compromise and publication of their Personal and Medical Information to unauthorized third parties; (iv) lost opportunity costs associated with effort expended and the loss of productivity

addressing and attempting to mitigate the actual present and future consequences of Defendant's conduct and the continued risk to their Personal and Medical Information, which remain in Defendant's possession, custody or control and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal and Medical Information of Plaintiffs and Class members; and (v) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal and Medical Information compromised by Defendant's conduct.

188. Plaintiffs and Class members have no other adequate remedy of law in that, absent injunctive relief from the Court, Defendant are likely to not fully redress the issues raised by their illegal and unfair business practices. Defendant has not announced any specific changes to its , processes or procedures to fix the vulnerabilities in the electronic information security systems and security practices, nor have they provided prompt and fully accurate notice of the circumstances surrounding this practice Thus, there is a real, credible threat of future harm either in terms of the continued misuse of the data that Defendant failed to protect.

189. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs seek an order of this Court for themselves, Class members, and for the benefit of the public granting injunctive relief in the form of requiring Defendant to correct its illegal conduct, to prevent Defendant from repeating the illegal and wrongful practices as alleged above and protect and preserve confidentiality of Personal and Medical Information in Defendant's possession that has been accessed, downloaded, exfiltrated, and viewed by at least unauthorized third party (i.e., Meta and other similar companies) because of Defendant's illegal and wrongful practices set forth above. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs also seek an order of this Court for equitable and injunctive relief in the form of prohibiting Defendant from continuing to refuse publicly issuing comprehensive direct and corrective notices as well as restitution and restitutionary

disgorgement of the monies Defendant saved and made from third party platforms and advertisers, in which Plaintiffs have a vested interest.

190. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiffs in relation to Plaintiffs' stake in the matter. Because this case is brought for the purposes of enforcing important rights affecting the public interest, Plaintiffs also seek the recovery of attorneys' fees and costs in prosecuting this action against Defendant under Cal. Code Civ. Proc. § 1021.5 and other applicable law.

DEMAND FOR RELIEF

Plaintiffs, both individually and on behalf of the Class and for the benefit of the public, pray for orders and judgment in favor of Plaintiffs and against Defendant as follows, as may be applicable to the Causes of Action set forth above:

- Finding that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;
- Designating Plaintiffs as representatives of the Class and listed counsel as Class counsel;
- Declaring Defendant's conduct in violation of the laws set forth above, including Cal. Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29, Cal. Bus. and Prof. Code §§ 17200 et seq., Cal. Bus. and Prof. Code §§ 22575-2257, Cal. Penal Code § 630-632 et seq., and Article I, § 1 of the California Constitution.

An order:

- prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- prohibiting Defendant from failing to protect, including through

encryption, all data collected through the course of their business operations in accordance with all applicable regulations, industry standards, and federal and state laws;

- prohibiting Defendant from refusing to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal and Medical Information of Plaintiffs and Class members;
- prohibiting Defendant from refusing to audit, test, and train security personnel regarding any new or modified procedures;
- prohibiting Defendant from refusing to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;
- All appropriate actual, compensatory, statutory, punitive, and other forms of damages as appropriate and permitted under the causes of action set forth above;
- All appropriate equitable monetary relief;
- Awarding Plaintiffs' counsel reasonable attorneys' fees and non-taxable expenses;
- Awarding Plaintiffs costs;
- Awarding pre-and post-judgment interest at the maximum rate permitted by applicable law; and,
- Granting such further relief as the Court deems just.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Date: March 10, 2023

DOYLE, APC

By: /s/ Chris W. Cantrell

William J. Doyle, SBN 188069
bill@doyleapc.com
Chris W. Cantrell, SBN 290874
chris@doyleapc.com
DOYLE APC
550 West B St, 4th Floor
San Diego, CA 92101
Phone: (619) 736-0000

April M. Strauss, SBN 163327
Astrauss@sfaclp.com
APRIL M. STRAUSS, APC
2500 Hospital Drive, Bldg 3
Mountain View, CA 94040
Phone: (650) 281-7081

Attorneys for Plaintiffs